La protection adéquate

Poullet, Yves

Published in:
XIXe Conférence internationale des commissaires à la protection des données

Publication date:
1997

Document Version
le PDF de l'éditeur

YP. 27c

19e Internationale conferentie	19th International Conference	19ème Conférence Internationale
Commissarissen Bescherming Persoonlijke Levenssfeer	Privacy Data Protection Commissioners	Commissaires à la Protection des Données
Brussel, België 17-19 september 1997	Brussels, Belgium 17-19 September 1997	Bruxelles, Belgique 17-19 septembre 1997

La protection adéquate dans les flux transfrontières de données

Professeur Yves Poullet,
Commission de la protection
de la vie privée, Belgique

19th International Conference of Privacy Data Protection Commissionners

[Conference] [Program] [Subjects] [Papers]

LA PROTECTION ADÉQUATE
Quelques réflexions à propos de l'article 25 de la directive européenne de protection des données

par Yves POULLET, Membre de la Commission belge, Professeur à la Faculté de Droit, Directeur du CRID des FUNDP (Namur)

P.S. L'exposé reprend la sutrcture d'une étude réalisée par le Centre de Recherches Informatique et Droit (C.R.I.D.) pour la DG XV de la Commission européenne. Un résumé de cette étude sera incessamment publié.

[l'article 25 de la directive - contexte - premier essai de comprehension] [le prealable: l'analyse des facteurs de risque] [une protection adequate] [une demarche d'evaluation] [au-dela de l'article 25: les articles 4 et 26 de la directive] [Notes]

I. L'ARTICLE 25 DE LA DIRECTIVE — CONTEXTE — PREMIER ESSAI DE COMPREHENSION

La dimension internationale des flux d'informations y compris nominatives, rendrait vain l'existence d'une réglementation dont l'effectivité couvrirait le seul territoire européen. Les autoroutes de l'information que préfigure la toile d'Internet favorisera encore cette circulation sans frontières, qu'il s'agisse de flux liés à la mobilité des personnes, de flux liés à un commerce électronique croissant ou à la consultation de sites étrangers, de flux, ou enfin, de flux liés à des transmissions soit propres à un groupe d'entreprises, soit à l'intérieur d'un secteur, soit intersectoriels.

Cette réalité risque de mettre à mal la protection des données garantie par la directive européenne. Cette dernière entend dès lors réglementer les flux transfrontières: elle le fait naturellement en assortissant de conditions les flux de données hors Europe (articles 25 et 26), elle le fait, exceptionnellement, en soumettant le responsable situé hors du territoire européen aux prescrits de la directive européenne (article 4.1.c). Ces deux types de dispositions font l'objet des développements suivants.

A. Le texte des alinéas 1 et 2 de l'article 25 - Des caractéristiques de l'approche à la notion de similalité fonctionnelle

En vertu de l'article 25.1. de la directive, "les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat". Le principe est donc l'interdiction du transfert; sauf à démontrer le caractère adéquat de la protection offerte dans le pays tiers.

La directive précise ensuite en son article 25.2 que l'appréciation du caractère adéquat de la protection du pays tiers doit tenir compte de "toutes les circonstances relatives à un transfert ou à une catégorie de transferts" et en particulier de différents facteurs, dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination, et certains concernent le niveau de protection dans le pays tiers, comme les règles de droit générales ou sectorielles en vigueur ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées".

Au-delà de ces réflexions, la notion de "protection adéquate" conduit à une approche - qui, à la lecture du texte de l'article 25, se caractérise comme suit:

- une approche au cas par cas, c'est-à-dire que la situation de la protection des données dans un pays tiers est évaluée "par rapport à un transfert déterminé ou une catégorie de transferts". L'article 25 al. 1 et al. 2 consacre, nous l'avons dit (supra n° 6), une approche au cas par cas, flux par flux ou catégorie de flux par catégorie de flux. Une telle analyse est évidemment lourde pour les Etats membres et les articles 25.4. et 25.6. mentionnent deux possibilités pour la Commission de leur simplifier le travail. Il s'agit de constater "conformément" à la procédure prévue à l'article 31 § 2 qu'"un pays tiers assure ou n'assure pas un niveau de protection adéquat". En d'autres termes, ces paragraphes permettent la constitution de "white" ou de "black" lists", décision valable pour des catégories de transferts, pour un secteur voire pour l'ensemble des flux vers un pays tiers.
- une approche souple et ouverte puisque selon le libellé même de l'article 25.2 l'évaluation doit pouvoir tenir compte à la fois des particularités propres et évolutives des divers flux transfrontières mais également des solutions diverses et évolutives que chaque Etat, voire chaque responsable des données, peut apporter, l'article 25 § 2 étant purement indicatif à ce propos. L'instrument méthodologique doit refléter cette ouverture et cette souplesse , et être adaptable aux multiples cas rencontrés ou à rencontrer;
- une approche fonctionnelle, c'est-à-dire que la protection s'évalue tant par rapport aux risques d'atteinte à la protection des données, risques générés par le flux en question, que par rapport aux mesures spécifiques ou générales mises en place par le responsable des données dans le pays tiers pour pallier ces risques.

L'évaluation de ces mesures doit se faire sans a priori; il ne peut être question d'imposer les mécanismes européens mis en place selon la directive (pas d'impéralisme européen) mais bien d'apprécier dans quelle mesure les objectifs de protection poursuivis par la directive sont rencontrés, de façon originale ou non par un pays tiers. En ce sens, la notion de protection adéquate ne représente en aucune manière un affaiblissement de la protection des données des personnes protégées au départ de la directive. Au contraire, elle crée pour

l'évaluateur la nécessité, tout en ne perdant pas de vue les exigences qui fondent selon la directive le besoin de protection, de prendre en considération les adaptations originales des modalités de cette protection, adaptations proposées par les pays tiers. L'instrument méthodologique doit laisser la place à cette variabilité de nature et de portée des solutions apportées, à cette recherche de "similarité fonctionnelle".

La "similarité fonctionnelle" implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans le pays tiers, mais bien la présence de tout élément remplissant les fonctions recherchées, même si les dits éléments doivent être d'une nature différente de ceux que l'onc connaît en Europe. Elle permet sans doute un meilleur respect des structures et des caractéristiques juridiques locales qu'un requis de protection équivalente, qui exige une similarité complète, législative en tout cas

B. La notion d'adéquation: premiers éléments

Quelques remarques liminaires s'imposent d'emblée au sujet de la notion d'"adéquation", que d'aucuns ont opposé à celle d'"équivalence" [1].

- Tout d'abord, cette notion suppose sans doute un référent (qui permette de répondre à la question: "par rapport à quoi la protection doit-elle être adéquate"?). Or, ce référent n'est pas défini comme tel par la directive. Il n'existe pas de système de référence déterminé par rapport auquel on puisse évaluer, la protection du pays tiers.

- Ensuite, on note que, si les critères énoncés par l'article 25.2 constituent de précieuses indications quant aux éléments à prendre en compte pour évaluer l'adéquation de la protection du pays tiers, ils ne constituent pas une liste exhaustive (l'article 25.2 énonce qu'il faut "en particulier" prendre en considération tel ou tel élément). On peut prendre en compte bien d'autres facteurs pour affiner cette analyse, que ces facteurs soient relatifs au flux considéré ou à la protection existant dans le pays tiers.

- Troisièmement, le contenu de ces éléments n'est pas défini: si par exemple on sait qu'il faut prendre en compte la durée des traitements, la directive n'indique pas plus avant ce qui serait une durée acceptable ou non. De même, le texte communautaire ne détaille pas ce que devraient être le "contenu minimum" d'une législation ou encore ses conditions d'application, pour considérer qu'elle assure un niveau adéquat de protection. On ajoutera que certains éléments énoncés se réfèrent aux caractéristiques du flux et désignent des facteurs de risques, alors que d'autres désignent la qualité des instruments de protection mis en place dans le pays tiers.

- Enfin, à propos des instruments de protection mis en place, l'article 25 se réfère non seulement aux normes issues de l'autorité publique qu'elles soient générales ou sectorielles mais également à des codes de conduite voire à des mesures techniques pourvu que ces instruments soient "respectées". Ainsi l'autorité de protection sera plus attentive à l'"effectivité d'un instrument, qu'à sa nature: ce qui importe, c'est qu'elle soit convaincue que l'instrument même s'il s'agit d'une simple "Company Privacy Policy" soit largement diffusé parmi les personnes concernées et les responsables des fichiers et puisse faire l'objet de recours des premiers vis-à-vis des seconds en cas de non respect par ceux-ci.

II. LE PREALABLE: L'ANALYSE DES FACTEURS DE RISQUE

A. Des définitions :

L'évaluation réclamée par l'article 25 prend en considération les risques propres à un flux ou une catégorie de flux, en fonction des dommages potentiels susceptibles d'être subis par la personne concernée. Cette prise en considération exige la détermination préalable des facteurs de risques qui permettront l'évaluation. En d'autres termes, 3 notions semblent importantes à définir: le risque, le dommage et le facteur de risque.

- le risque est un événement dont la survenance n'est pas certaine mais entraîne pour la personne fichée un dommage.

  En matière de protection des données, quatre catégories de risques sont susceptibles d'intervenir :
  - de perte de contrôle,
  - de réutilisation des données,
  - de manque de proportionnalité,
  - d'inexactitude de ces données.
- Les dommages, quant à eux peuvent être d'ordre immatériel, matériel ou encore concerner la sécurité physique des personnes, sans qu'à cet égard, l'on puisse procéder à une "échelle" des dommages suivant leur gravité et réserver la protection des données aux dommages de la seconde et troisième catégorie.
- Par "facteur de risque", on entend tous les éléments propres à un transfert ou une catégorie de transferts qui, chacune, sont susceptibles d'avoir une influence positive ou négative sur la probabilité de réalisation du risque.

Enfin, on souligne la nécessité d'appliquer à chaque facteur de risque, un "coefficient pondérateur" élément susceptible de renforcer ou diminuer l'importance des facteurs de risque: il s'agit de ce que l'on appelle la "différence culturelle". Ainsi, les tradition propre à un pays de cessions de fichier au secteur marketing y accroissent le risque de réutilisation des données; certains pays peuvent considérer les données syndicales comme non sensibles, etc.

B. Tableau d'analyse des facteurs de risques

Parmi les facteurs de risque, certains sont particuliers aux flux transfrontières (situation politique ou

technologique du pays tiers, fait que les données sont rarement collectées directement auprès de la personne concernée); d'autres sont généraux c-à-d liés à toute forme de transfert de données (nature des données, type de transfert, ...).

- Particuliers aux FTD

	Risques				
Facteurs de risques particuliers aux FTD	Perte de contrôle	Réutilisation	Manque de proportionnalité	Inexactitude des données	Observations
Situation socio-politique		* [2]			
Retard technologique	*	*			
Technologie avancée		*			
Collecte indirecte des données	*	*			
Réexportation des données [3]	*	*			

- généraux

Facteurs de risques généraux [4]	Risques				
	Perte de contrôle	Réutilisation	Manque de proportionnalité	Inexactitude des données	Observations
Sensibilité des données			*		
Nombre de renseignements transférés			*		
Nombre de personnes concernées	*				
Fréquence des flux		*		*	
Type de transfert utilisé	*	*			
Localisation du fichier central	*				
Liens entre acteurs	*				
Secteur d'activité du destinataire	*	*			
Cohérence dans les finalités	*	*			
Durée de conservation des données		*	*	*	
Détermination de la finalité	*	*			

III. UNE PROTECTION ADEQUATE

A. Le référent

a. Les principes de fond

L'existence des principes de fond se déduit de la volonté essentielle de tout instrument de protection des données d'assurer à l'individu une maîtrise de la circulation de son image informationnelle et de son utilisation (principes de participation individuelle et de finalité) et de leur volonté complémentaire de permettre un contrôle des caractéristiques de cette image informationnelle dans sa qualité (principe de qualité) et son ampleur (principe de proportionnalité).

Le principe de participation individuelle exprime la nécessité de permettre par divers moyens à la personne concernée d'obtenir une information sur "l'image informationnelle" que le responsable du traitement a de lui et, dès lors, d'exercer vis-à-vis de cette image un certain contrôle voire une certaine maîtrise.

Le principe de finalité exige la limitation de l'utilisation de données à caractère personnel aux seuls traitements dont les finalités sont compatibles avec les finalités légitimes qui ont été déterminées et rendues explicites de leur collecte initiale.

Le principe de proportionnalité implique de limiter dans la durée, en quantité et en qualité les données traitées aux seules données nécessaires à la poursuite des finalités légitimes.

Le principe de qualité induit la recherche d'exactitude et de mise à jour des données personnelles dans la mesure exigée par la finalité.

b. La conception de ces principes dans la directive

- l'exigence de "légitimité" de la finalité ce qui suppose: un "certain" contrôle social;
- la participation individuelle comme principe à géométrie variable.

B. L'effectivité du respect des principes de fond

a. Une diversité de moyens de protection

+ les moyens d'expression

On s'interroge sur l'origine, le mode écrit ou non qui exprime la protection: la valeur du moyen d'expression dépendra de l'auteur de ce moyen et de son caractère plus ou moins obligatoire et contraignant

Source d'expression	Qui exprime?	Renvoi possible à d'autres moyens d'expression
Privacy Policy	Entreprise	Certifications, codes de conduite
Certification	Organe de standardisation	Règles normatives prises par l'autorité publique
Codes de conduite	Organe sectoriel	Règles normatives issues de l'autorité publique
Règles normatives issues de l'autorité publique	• constitution • pouvoir législatif • gouvernement • Board	Tous les autres hormis le contrat

+ Les moyens de contrôle:

c'est-à-dire l'ensemble des méthodes combinées ou non qui ont fonction directe ou indirecte, exclusive ou non de garantir le respect des principes.

Moyen de contrôle	Mis en place par	Exercé par
Mesures de sécurité	Responsable du traitement	Responsable du traitement le cas échéant, contrôle en outre par: • entreprise tierce spécialisée • organe sectoriel • autorité de contrôle
Autorité indépendante de contrôle	Autorités publiques	Autorité indépendante de contrôle
Accès	Responsable du traitement	Personne concernée (exceptionnellement par une autorité de contrôle)
Détaché à la protection des données	Responsable du traitement	Détaché à la protection des données
Représentant	Responsable du traitement	Entreprise soit représentante, soit tierce
Audit	Responsable du traitement	Entreprise tierce spécialisée Autorité indépendante de contrôle
Notification	Autorité de contrôle Organisme privé	Autorité de contrôle Organisme privé + contrôle collectif diffus

+ les moyens de recours et de contrainte

Par moyens de sanction des principes de fond, on entend, au sens large, les divers modes et procédures de dissuasion, de réparation ou de répression mis en place pour combattre les déviances par rapport aux comportements attendus pour assurer le respect des principes de fond.

Nous proposons de distinguer les sanctions selon leurs auteurs.

Auteurs	Sanctions	Dimension
Organe de standardisation ou de certification	Refus ou retrait d'un certificat	Nature commerciale
Secteur	Recommandations Blâme, amendes, retrait de l'association	Nature commerciale Effets sectoriels si publication Effets vers le public
Autorité de contrôle	Recommandations Destruction de données Interdiction de traitements Avis préalable	Nature commerciale avec effets sectoriels Si publication, effets vers le public
Juridictions administratives	Destruction de données Interdiction de traitements Amendes	Nature administrative Effets vers le public
Juridictions civiles	Réparation du dommage Mesures de réparation en nature Publication du jugement	Nature judiciaire Effets vers le public
Juridictions pénales	Amendes, emprisonnement	Nature judiciaire

	Réparation du dommageSaisie et destruction Publication du jugement	Effets vers le public

b. Quelques règles

Règle 1: chaque moyen doit être analysé dans sa logique propre et en en fonction du contexte du système juridique dans lequel il apparaît. A nouveau apparaît ici l'importance du coefficient pondérateur dit de "différence culturelle".

Règle 2 : Chaque moyen renvoie à ses propres conditions d'effectivité dont le respect devra être établie.

Règle 3 : Le résultat à atteindre dépend non d'un seul moyen mais toujours d'une combinaison de moyens d'expression, de contrôle, de recours et de sanction.

Règle 4 : La combinaison des moyens proposés doit nécessairement garantir le respect non d'un seul principe mais en particulier des deux principes essentiels: ceux de la participation individuelle et de la finalité.

c. Des conditions minimales d'effectivité

Condition 1: L'"awareness" des principes

Condition 2: Le droit d'accès et de correction

L'effectivité des moyens de contrôle et de sanctions pour la personne européenne concernée suppose, en tout cas, la reconnaissance directe ou indirecte de droits d'accès et de contestation faciles à exercer devant une juridiction et ce peu importe la technique d'expression choisie.

Condition 3: Les mesures de sécurité appropriées

Condition 4: Une autorité indépendante de contrôle:

The "right not to be let alone" est déjà consacré par la directive sur le territoire européen. Il doit l'être bien plus encore lorsque la personne concernée voit ses données traitées dans un pays dont elle ignore la culture, la langue, etc. Cette condition implique l'existence d'une autorité de contrôle accessible, agissant de manière indépendante et caractérisée par l'exercice de certaines fonctions.

Chaque caractéristique mérite quelques développements

- l'accessibilité de l'autorité se conçoit tant par l'annonce auprès des personnes concernées de son existence, que par sa saisine aisée.
- l'action indépendante de l'autorité suppose une liberté d'action par rapport aux intérêts du ou des responsables de traitement. Elle se déduit de divers facteurs (composition de l'organe, transparence du fonctionnement, moyens d'investigation, caractère public du rapport d'activités).
- quant aux fonctions de cette autorité, elles consistent non seulement en la promotion des principes auprès des responsables, l'assistance des personnes concernées dans l'accès et la contestation, le contrôle du respect des principes auprès des responsables du traitement [5].

Condition 5: "Risques de retransfert": l'exigence d'une protection adéquate par transitivité

IV. UNE DEMARCHE D'EVALUATION

A. Le rassemblement des informations nécessaires à l'évaluation

- Quelles informations rassembler?

  Deux questionnaires, permettant

  - l'identification des risques, d'une part
  - l'identification des moyens de protection, d'autre part.

- Auprès de qui rassembler les informations ?
  - auprès de l'émetteur
  - auprès du destinataire en cas de collecte directe auprès de lui
  - auprès de tiers: le "rating agencies"

B. L'analyse des informations rassemblées

- La prise en compte du coefficient "différence culturelle". Un exemple: une" privacy policy" constitue-t-elle des "statements" dont le non respect ouvre un droit de recours juridictionnel facile et

aisé dans le système américain?
- Le système des "rating agencies" agréées par les autorités européennes de protection des données et appelées à intervenir pour la prise en compte du coefficient "différence culturelle"

C. La décision

- et les facteurs de risques
  - Comment jouer sur un facteur de risque!
  - l'identification des principes de fond mis en cause par les facteurs de risque
- et les moyens de protection

La démarche pourrait se résumer comme suit:

a. Moyens d'expression

Il faut, pour chaque principe retenu, déterminer par quel moyen il est exprimé: code de conduite, norme établie par l'autorité publique, etc,...

Pour être retenu, chacun de ces moyens d'expression doit:

- être créateur de droits pour les personnes concernées (voir supra, chapitre III);
- être créateur de droits pour les personnes concernées (voir supra, chapitre III);
- quant à son contenu, faire l'objet d'une information large auprès des responsables de traitement et des personnes concernées;
- s'appliquer aux étrangers non résidents sur le territoire du pays tiers (et en particulier, aux ressortissants de l'Union européenne);

b. Moyens de contrôle

Chaque principe de fond retenu doit voir son effectivité assurée également par des moyens de contrôle. Les moyens de contrôle à rechercher sont, dans tous les cas, ceux qui font partie du "noyau dur de l'effectivité". Il s'agit de mesures de sécurité, de l'existence d'une autorité indépendante de contrôle et de mesures garantissant l'accès des personnes concernées à leurs données.

L'analyse du flux permet de déterminer de façon plus précise quel niveau d'exigence est souhaitable pour admettre ces moyens; elle permet également de déterminer si d'autres moyens de contrôle doivent être exigés. Ainsi, si le flux analysé est un flux "marketing", l'accès des personnes concernées devra leur permettre non seulement de vérifier les données les concernant, mais encore de s'opposer (opt out) au traitement. Si le pays tiers est affecté d'un retard technologique important, il importe que les mesures de sécurité prises par le responsable du traitement tiennent compte de ce facteur. Si le risque de perte de contrôle est accentué par de nombreux facteurs tenant essentiellement à l'éloignement et la difficulté d'atteindre le maître du fichier, la nomination d'un "représentant" sera sans doute nécessaire.

On le voit, il est difficile de dresser un tableau de toutes les combinaisons de moyens possibles: elles sont fonctions d'éléments propres au flux considéré, et sont également influencées par la "différence culturelle". Cependant, il est vraisemblable que la pratique permette de dégager plus systématiquement des moyens ou combinaisons de moyens particulièrement adaptés pour tel ou tel type de flux.

c. Moyens de recours et de sanctions

Il faut ensuite voir à quels moyens de recours et de sanction le moyen d'expression renvoie: s'agit-il d'un moyen de recours particulier à ce moyen d'expression, ou renvoie-t-il plus généralement aux recours judiciaires? Ici aussi, il faudra pour chaque cas analyser l'effectivité des moyens de recours et de sanction. Peu importe leur nature, les moyens de recours doivent d'une part, assurer le droit des personnes concernées à une procédure contradictoire d'accès aisé devant un organe juridictionnel disposant d'une compétence d'exécution de ses décisions. Quant aux moyens de sanction, ils doivent être suffisants pour faire craindre au responsable du traitement un dommage supérieur au bénéfice qu'il tire du non respect des principes. Chaque principe de fond doit être assorti de moyens de recours et de sanction. Cela implique que l'autorité en charge du contrôle pourrait considérer la protection du pays tiers comme inadéquate si aucune sanction appropriée n'est prévue pour l'un ou l'autre principe.

V. AU-DELA DE L'ARTICLE 25: LES ARTICLES 4 ET 26 DE LA DIRECTIVE

A. L'article 26 de la Directive: les exceptions au requis de la protection adéquate

La directive "sous réserve de dispositions contraires de leur droit national régissant des cas particuliers [6], édicte certaines exceptions au principe de l'article 25 et autorise ainsi des transferts de données à caractère personnel vers des pays n'offrant pas un niveau de protection adéquat. Deux types d'exception sont prévus: le premier vise certaines catégories de flux; le second vise la substitution à un mode adéquat de protection, d'un mode 'ad hoc" de protection : le contrat.

A propos de la première catégorie d'exceptions, l'article 26.1 vise notamment lorsque la personne concernée a

indubitablement donné son consentement à l'opération de transfert (article 26.1a). On ne peut parler de véritable consentement que si celui-ci est "éclairé" [7] c'est-à-dire si la personne concernée a conscience qu'il s'agit bien d'un flux transfrontalier, connaît le pays de destination des informations qu'elle transmet et réalise que ce pays n'assure pas un niveau de protection adéquat des données. D'autres exceptions existent. Elles reprennent les hypothèses prévue par l'article 7 pour légitimer un traitement à l'exception de celle visée à l'article 7f: soit le transfert nécessaire à l'exécution d'un contrat ou à l'exécution de mesures précontractuelles, soit entre la personns concernée et le responsable du traitement, soit entre le responsable du traitement et un tiers dans l'intérêt de la personne concernée, soit le transfert sert à la sauvegarde d'un intérêt vital ou d'intérêt public important ou s'opère dans le cadre d'une action en justice.

On notera qu'il importe que le transfert soit nécessaire au regard de tels intérêts et qu'il ne suffit pas que l'intérêt contractuel existe pour que le transfert soit autorisé [8]. Ainsi, dans le cadre d'une multinationale, la création en terre lointaine d'une banque de données relative à l'ensemble des travailleurs et les flux engendrés à partir des filiales européennes ne pourront bénéficier de l'exception de l'article 26 que si le responsable démontrer qu'il existe une nécessité d'opérer ce transfert pour l'exécution du contrat. Sans doute, cette nécessité n'existera que pour quelques employés appelées par exemple à une grande mobilité au sein de la firme et à leur propos uniquement pour quelques données, et non pour des données de base [9].

La seconde catégorie d'exceptions entend substituer à des modes adéquats de protection, ceux palliatifs envisagés par le responsable dans le cadre d'un contrat régissant un flux ou plusieurs flux. Ainsi, si le secteur marketing d'un pays tiers n'offre pas de protection adéquate aux données originairement protégées par la Directive, une ou plusieurs entreprise(s) (voire une association de sociétés de marketing) peuvent prendre dans le cadre des contrats couvrant les flux transfrontières en provenance d'Europe, des engagements supplémentaires, par exemple en limitant les finalités de réutilisation des données. ouvrant le droit d'opposition et finalement en permettant à une autorité de protection des données d'inspecter leurs traitements. A propos de ce second type d'exception, une autorisation de l'Etat membre est nécessaire. Cette autorisation suppose la vérification du caractère "suffisant" des garanties offertes. L'Etat membre informe la Commission de telles autorisations et des oppositions exprimées par d'autres Etats membres sont possibles. On souligne à ce propos, le rôle important joué par la Commission qui peut, après délibération des représentants des Etats membres, imposer une décision aux Etats membres, soit l'acceptation de telles mesures palliatives, soit leur rejet ou la proposition de mesures supplémentaires.

B. Applicabilité extraterritoriale de la Directive.

Selon l'article 4 c) de la directive, le droit national pris en application de la directive s'applique: "lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire dudit Etat membre". L'article 4.2. ajoute que l'applicabilité du droit national entraîne l'obligation pour le responsable de désigner un représentant établi sur le territoire de l'Etat membre.

Le critère de rattachement affirmé par le texte est donc le "recours" à des moyens automatisés ou non situés sur le territoire de l'Union européenne. La notion est vague. Prise au sens large, elle consacrait des hypothèses où la collecte des informations opérée par exemple en Belgique est suivie par un transfert des données vers l'étranger pour y être traitées par exemple à meilleur prix mais également l'interrogation d'une banque de données sise en Belgique, dans laa mesure où l'interrogation propre à la banque de données, elle étendrait même l'applicabilité de la directive un système de réservation aérienne dans la mesure où interrogeant une boite aux lettres tenue à sa disposition en Europe par une agence de voyage, il prend connaissance de messages EDI qui lui sont destinés.

Bref, l'interprétation large de la notion de "recourir" aboutirait à décréter que la quasi totalité des flux transfrontières amènerait le destinataire des flux à tomber sous le champ d'application de la directive. Point ne serait besoin alors des dispositions des articles 25 et 26 de la directive, puisqu'en toute hypothèse la directive serait applicable.

Lors d'une analyse récente de l'application de la directive à Internet, M-H. Boulanger et C. de Terwangne [10] ont proposé une autre interprétation qualifiée de "téléologique" du critère de rattachement proposé par l'article 4.1.C). Nous en reproduisons le texte: "La ratio legis de cet article se résume clairement dans la volonté d'éviter que les individus se trouvent dépourvus de toute protection, en particulier du fait d'un contournement de la législation. Le souci des auteurs du texte est donc d'assurer une protection à ceux qui doivent normalement en bénéficier sous l'égide de la directive, même en dehors des frontières communautaires.

C'est par une lecture combinée de l'article 4.1.c et des articles 25 et 26 qui régissent les flux transfrontières vers les Etats tiers qu'une définition rationnelle de l'applicabilité de la directive pourra être dégagée.

On peut, en effet, considérer qu'une première réponse à la préoccupation des auteurs de la directive est donnée par l'instauration d'un régime protecteur en matière de flux transfrontières de données vers les pays tiers à la Communauté. Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi européenne s'imposent à tous les acteurs qui effectuent des opérations sur des données fournies à l'étranger en provenance de l'Union.

La réponse contenue dans l'article 4.1.c) vise à couvrir, quant à elle, les situations dans lesquelles les sujets des données se voient privés, par une manoeuvre artificielle, du bénéfice de la protection de l'ensemble de la directive, et les situations échappant à toute protection, même celle instaurée en matière de flux transfrontières. Dans ce sens, deux catégories de situations entrent, selon nous, dans le champ de l'article 4.1.c:

- celle précisément où un responsable de traitement cherche délibérement à contourner la directive et, pour ce faire, délocalise son établissement vers un pays tiers, tout en faisant usage de moyens localisés

sur le territoire communautaire pour réaliser son traitement.
- celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers.

Ainsi un logiciel permettrait à un responsable sis à l'étranger de visiter l'ensemble des forums de discussions mis en place par des serveurs européens et d'y repérer les interventions de telle ou telle personne afin de constituer son profil de personnalité.

En conclusion, l'article 4.1.c) couvre des hypothèses exceptionnelles soit celles où la localisation du responsable est anormale au regard de son action orientée vers l'Union européenne et déterminée par des données en provenance de celle-ci, soit celles où est déjouée la protection offerte par la réglementation des flux transfrontières dans la mesure où ce flux est généré par la seule activité de la personne située à l'étranger sans qu'il y ait à proprement parler communication c'est-à-dire action de transfert de données, d'un responsable de traitement situé dans le territoire de l'Union européenne. Cette seconde hypothèse vise en particulier les flux générés par les traitements invisibles (cookies, applets Java, etc.) liés à l'utilisation des navigateurs sur Internet.

Notes

1. La notion de protection équivalente est utilisée par la Convention du Conseil de l'Europe, dite Convention n° 108 en son article 12. Cet article met à charge d'une partie contractante une obligation de permettre les flux vers les autres Etats partie à la même convention si cet Etat assure une protection équivalente. On notera que la notion d'équivalence de protection ne règle que les flux entre pays ayant ratifié la Convention du Conseil de l'Europe et non vers les pays tiers. A propos de cette différence, A. Bourlond, Y. Poullet, Flux transfrontières de données à caractère personnel, position de la proposition de directive européenne face à celle de la convention 108 du Conseil de l'Europe, D.I.T., 1991/2, p. 58 et s.
[Back to text]
2. Les signes seront remplacées par un signe + ou - selon que le risque est augmenté ou diminué lors de l'analyse d'un flux concret.
[Back to text]
3. Le facteur de risque "réexportation de données" est important, en particulier, on peut craindre que la protection offerte par un pays tiers vers lequel le flux originaire de données se situe, soit illsoire dans la mesure où l'entreprise destinatoire réexporte les données vers d'autres pays cette fois sans protection adéquate. La présence de ce facteur de risque peut se déduire d'une variété d'autres facteurs, ainsi si l'entreprise destinataire n'est que la filiale d'une entreprise localisée ailleurs, est un simple service bureau voire des pratiques habituelles de cessions de fichiers propres à une région du globe.
[Back to text]
4. c'est-à-dire valables pour tout flux qu'il soit transfrontière ou non.
[Back to text]
5. Cette conception fonctionnelle large de l'autorité de contrôle se distingue de celle institutionnelle (conception présente dans la directive). Elle permet de considérer comme autorité indépendante de contrôle, un organe de médiation créé au sein d'une fédération professionnelle à condition qu'il remplisse les 3 conditions détaillées ci-dessus (accessibilité, indépendance, fonctions).
[Back to text]
6. "Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat (...) peut être effectué (...) (Article 26.1). "Les Etats membres peuvent donc, par des dispositions régissant des cas particuliers, refuser que l'une ou l'autre exception s'applique à ces cas. On pense dans un premier temps aux situations mettant en jeu des données sensibles, médicales ou judiciaires. Mais la particularité des cas retenue peut être plus large et consister non plus dans le caractère sensible des données mais, par exemple, dans la nature du réseau - ouvert ou fermé - utilisé. On peut donc imaginer qu'un Etat membre soit plus strict qu'un autre en matière d'exceptions appliquées à l'utilisation d'un réseau Internet" (M-H. Boulanger, C. De Terwangne, Internet et le respect de la vie privée, in Internet face au droit, E. Montero (éd.), Cahier du CRID n°12, Bruxelles, Story-Scientia, 1997, p. 211). L'inteprétation donnée par les auteurs cités est ainsi large. La notion de "cas particulier" pourrait s'interpréter comme laissant seulement la possibilité pour l'autorité antionale d'intervenir pour un flux déterminé et de déroger exceptionnellement et non par catégorie aux différentes hypothèses prévues par l'article 26.
[Back to text]
7. Sur cette notion, cf. supra n° ...
[Back to text]
8. L'article 26 constituant une exception doit s'interpréter de manière stricte, nous semble-t-il...
[Back to text]
9. Par exemple, les données d'administration des salaires...
[Back to text]
10. H. Boulanger, C. de Terwangne, o.c., p. 202. Les auteurs se réfèrent également à la lecture du considérant n° 20 et à l'exposé des motifs de la première proposition de directive émanant du Conseil (Proposition du 15 oct. 1992, COM(92) 422 final - SYN 287, p. 13).
[Back to text]